BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT/SE 98/00897
09/423511

PRV
PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
C rtificat

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande* / *Applicant (s)* — *Acces Security Sweden AB, Grödinge SE*

(21) *Patentansökningsnummer* / *Patent application number* — *9701814-7*

(86) *Ingivningsdatum* / *Date of filing* — *1997-05-15*

PRIORITY DOCUMENT

Stockholm, 1998-06-02

För Patent- och registreringsverket
For the Patent- and Registration Office

Åsa Dahlberg

Avgift
Fee

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

ELEKTRONISK TRANSAKTION

Tekniskt område

Föreliggande uppfinning hänför sig allmänt till elektroniska transaktioner, dvs främst betalningar, som sker på elektronisk väg. Uppfinningen avser speciellt elektroniska transaktioner som sker under utnyttjande av ett användarkort, såsom ett bankkort, kreditkort, kontokort, eller dylikt, vilket kort är ett så kallat aktivt kort.

Teknisk bakgrund

Under senare år har intresset för elektroniska transaktioner ökat markant, särskilt i takt med att Internet fått ett kraftigt genomslag. Säkerhetsfrågor har härvid hamnat i fokus, och det har föreslagits olika system och standarder som skall garantera säkerheten i samband med elektroniskt översändande av transaktionsmeddelanden. Av särskilt intresse har varit hur man skall skydda exempelvis över Internet överförda kreditkortsnummer i samband med handel över Internet. Föreslagna system och standarder har det gemensamt att de bygger antingen på att känslig information, som kan missbrukas, t ex ett kreditkortsnummer, icke skall överföras över kommunikationsnätet, eller på att sådan känslig information skall överföras i krypterad form. I båda alternativen ligger tonvikten på förhållandevis komplicerade administrativa rutiner och systemkonfigurationer, etc, vilket såsom inses innebar begränsningar och hinder för ett mera allmänt utnyttjande.

Uppfinningens syfte

Ett huvudsyfte med föreliggande uppfinning är att möjliggöra elektroniska transaktioner på ett förenklat sätt under bibehållande av full säkerhet.

Ett annat syfte är att möjliggöra olika slags elektroniska transaktioner inom ramen för samma grundkoncept.

Ännu ett syfte är att möjliggöra elektroniska transaktioner oberoende av val av kommunikationsväg för utnyttjat transaktionsmeddelande.

Ytterligare ett syfte är att möjliggöra elektroniska transaktioner som i princip icke kräver överföring av utnyttjat transaktionsmeddelande via en säker kommunikationsväg.

Sammanfattning av uppfinningen

Ovannämnda syften uppnås genom de uppfinningssärdrag som framgår av bifogade patentkrav.

Uppfinningen baserar sig sålunda på en insikt om det fördelaktiga i att utnyttja speciella transaktionsmeddelanden, som oberoende och under full egen kontroll skapas av en användare och som har sådan beskaffenhet, att de endast kan ha skapats av användaren i fråga, icke kan ha manipulerats under översändande till en mottagare eller adressat utan att detta rätt kan konstateras (äkthetskontroll), och enkelt kan "valideras" efter översändare i och för slutförande av önskad transaktion. Enligt uppfinningen utnyttjar avsändaren ett honom tillordnat unikt aktivt kort med däri lagrad privat nyckel (vars publika motsvarighet i ett asymmetriskt kryptosystem är allmänt tillgänglig) för att förse ett av avsändaren skapad transaktionsmeddelande med en för avsändaren unik digital signatur, varefter det signerade transaktionsmeddelandet kan översändas på godtyckligt sätt.

Endast en rättmätig användare av det aktiva kortet kan aktivera detta för signering, varigenom ett grundläggande identitetskrav är uppfyllt. Den digitala signaturen innebär vidare ett datalås som omöjliggör meddelandemanipulering utan upptäckt vid senare äkthetskontroll med utnyttjande av den allmänt tillgängliga publika nyckel, som hör till användaren. Användarens oberoende skapande av transaktionsmeddelandet innebär full kontroll av innehållet i meddelandet. Uppfinningen innebär sålunda krav på koppling av känsliga uppgifter, såsom ett kortnummer, i det överförda transaktionsmeddelandet till en digital

signatur för att uppgifterna i fråga skall vara användbara. I avsaknad av en koppling till en digital signatur är uppgifterna sålunda i princip värdelösa och kan följaktligen icke missbrukas för falska nättransaktioner, även om det skulle kunna fångas upp av någon utomstående i samband med ett översändande av transaktionsmeddelandet. Hur översändandet sker blir i princip utan betydelse. Detta innebär ett synsätt som är helt motsatt dagens strävanden efter att åstadkomma särskilda, sakra, dvs krypterade, kommunikationssystem för översändande av transaktionsmeddelanden över exempelvis Internet.

Det är föredraget att ett transaktionsmeddelande enligt uppfinningen innehåller uppgift om avsändare, transaktionsbelopp och mottagare samt företrädesvis en föränderlig uppgift, såsom ett löpnummer.

Enligt uppfinningen skapar sålunda användaren vad som kan sägas vara en signerad "elektronisk check", vilken kan översändas på godtyckligt sätt och vid godtycklig tidpunkt till en adressat eller mottagare.

Efter mottagning kan ett transaktionsmeddelande enligt uppfinningen kontrolleras vad gäller äkthet genom kontroll av den digitala signaturen, varefter "validering" och gottskrivning eller kreditering av mottagaren med transaktionsbeloppet ifråga kan ske på godtyckligt lämpligt sätt, lämpligen enligt samma principer som gäller för inlösen av en vanlig check eller för clearing i samband med kortköp.

Enligt uppfinningen kan det översända, signerade transaktionsmeddelandet innehålla erforderliga transaktionsuppgifter i klartext, varvid den digitala signaturen på känt sätt kan vara beräknad på ett kondensat av meddelandeuppgifterna. Detta innebär att senare äkthetskontroll, validering och kreditering på mottagarsidan underlättas, eftersom erforderliga uppgifter direkt föreligger, såsom uppgift om avsändare, som gör det enkelt att hämta rätt publik nyckel i och för äkthetskontroll av den digitala signaturen.

Om den digitala signaturen utförs på hela transaktionsmeddelandet, så att detta överförs i krypterad form, kan det överförda transaktionsmeddelandet vara försett med särskild avsändaruppgift som gör det möjligt att på mottagarsidan hämta rätt publik nyckel för äkthetskontrollen och omvandling av transaktionsmeddelandet till klartext.

Enligt uppfinningen kan transaktionsmeddelandet innehålla avsändaruppgift av godtyckligt lämpligt slag, såsom åtminstone en av följande uppgifter: ett kortnummer, ett bankkortnummer, ett betalkortnummer, ett kreditkortnummer, ett kontonummer, ett fakturanummer och ett ID-nummer. Om det enligt uppfinningen utnyttjade aktiva kortet är ett till ett konto kopplat kort, såsom ett kreditkort, kan det vara föredraget att såsom avsändaruppgitt utnyttja tillhörande kortnummer. Såsom fackmannen inser är det dock möjligt att använda varje slags uppgift, som på mottagarsidan enkelt kan kopplas ihop med en användaridentitet och därigenom med ett tillhörande konto, som skall debiteras.

För mottagaruppgiften gäller i princip samma sak. Exempelvis kan det vara fråga om åtminstone en av följande uppgifter: ett kortnummer, ett bankkortnummer, ett betalkortnummer, ett kreditkortnummer, ett kontonummer, ett fakturanummer och ett ID-nummer. Även här är det tillräckligt att ifrågavarande uppgift på mottagarsidan entydigt kan relateras till en betalningsmottagare. Det skall påpekas att överförande av ett transaktionsbelopp till en mottagare inte behöver innebära att ett mottagarkonto krediteras, utan att det också kan vara fråga om att exempelvis en administrativ enhet, som mottager transaktionsmeddelandet, efter äkthetskontroll och validering debiterar ett avsändarkonto och till mottagaren sänder vad som kan betraktas som en check eller postanvisning.

Såsom tidigare redovisats är ett väsentligt särdrag hos föreliggande uppfinning att avsändaren, dvs användaren av det aktiva kortet, skapar och signerar transak-

tionsmeddelandet under egen kontroll, dvs i princip oberoende av uppkoppling mot ett kommunikationsnät och av en datadialog med en mottagare, ehuru en dylik dialog naturligtvis kan förekomma i samband med översändande av ett signerat transaktionsmeddelande. Transaktionsmeddelandet skapas följaktligen företrädesvis fristående från kommunikationsnätet eller off-line. Detta innebär att avsändaren har full kontroll över vilka uppgifter som inmatas för skapande av transaktionsmeddelandet. Signeringen kan såsom inses endast åstadkommas av avsändaren, eftersom denne i normalfallet är ensam om att kunna aktivera sitt aktiva kort och utlösa signeringen. När det gäller översändandet eller överlämnandet av det signerade transaktionsmeddelandet finns dock icke några restriktioner, såsom utan vidare inses. Exempelvis kan användaren eller någon denne behjälplig person ta med sig det aktiva kortet med det däri befintliga, signerade transaktionsmeddelandet för senare meddelandeavsändande, för meddelandeavsändande på annan plats, etc, dvs stor valtrihet råder. Det signerade transaktionsmeddelandet skulle också kunna föras över på ett särskilt mellanlagrings- eller transportmedium i och för overtöring till en mottagare och/eller adressat.

Enligt uppfinningen är det fördelaktigt att transaktionsmeddelandet skapas i det aktiva kortet. Transaktionsmeddelandet kan härvid lämpligen skapas med hjälp av i det aktiva kortet i förväg inlagd programvara och företrädesvis i kortet i förväg inlagd avsändaruppgift, t ex ett kortnummer. Lämpligen skapas också automatiskt ett nytt löpnummer för varje transaktionsmeddelande. Inmatning av erforderliga meddelandeuppgifter i kortet kan ske på olika sätt, t ex medelst på det aktiva kortet anordnade inmatningsorgan, varvid kortet med fördel utgörs av ett så kallat avancerat aktivt kort. För transaktionsmeddelandet erforderliga uppgifter kan också inmatas medelst en skyddad kortterminal, som med fördel kan utgöras av användarens egen kortläsartörsedda terminal eller da-

tor. För transaktionsmeddelandet erforderliga uppgifter kan också inmatas medelst en separat kortkommunikationsenhet, varvid den senare företrädesvis senare även fungerar såsom kortaktivator. En dylik enhet kan med fördel vara utförd som en liten, bärbar enhet, som användaren kan ha med sig och som av användaren utnyttjas då han vill aktivera sitt kort och/eller inmata uppgifter i kortet i en miljö, där någon skyddad kortterminal inte finns.

För transaktionsmeddelandet erforderliga uppgifter kan också inmatas medelst en av det aktiva kortet styrd telekommunikationsenhet, speciellt en mobil sådan, såsom en mobiltelefonanordning. I detta sammanhang kan enheten också utnyttjas för översändande av det signerade transaktionsmeddelandet, t ex med utnyttjande av en tjänst av så kallad SMS-typ.

Fackmannen inser att det även är möjligt att skapa själva transaktionsmeddelandet utanför det aktiva kortet exempelvis vid utnyttjande av något av ovannämnda uppgiftsinmatningsorgan. Det skapade transaktionsmeddelandet inmatas därefter i det aktiva kortet i och för signering.

Enligt en första aspekt på föreliggande uppfinning åstadkommes ett förfarande för genomförande av elektroniska transaktioner, varvid en avsändare av transaktionsmeddelanden tilldelas ett aktivt kort med tillhörande unik identitet och i kortet skyddat lagrad privat nyckel och varvid en tillhörande publik nyckel hålls allmänt tillgänglig, vilket förfarande utmärks av att avsändaren i samband med en elektronisk transaktion under egen kontroll, företrädesvis genom egen inmatning av meddelandeuppgifter, skapar ett transaktionsmeddelande, som innehåller för transaktionen erforderliga uppgifter, samt i sitt aktiva kort förser det skapade transaktionsmeddelandet med sin digitala signatur under utnyttjande av sin privata nyckel i och för senare utmatning och avsändande av transaktionsmeddelandet.

Enligt en andra aspekt på föreliggande uppfinning åstadkommes ett aktivt kort för genomförande av elektroniska transaktioner, vilket kort innefattar organ för lagring av kortidentifieringsuppgifter, organ för skyddad lagring av en privat nyckel, organ för lagring av en asymmetrisk algoritm, organ för inmatning av transaktionsuppgifter i kortet, processororgan för att i kortet skapa ett transaktionsmeddelande baserat på inmatade transaktionsuppgifter, såsom uppgifter som belopp och mottagare, och eventuellt i kortet lagrade uppgifter såsom uppgifter om avsändare och företrädesvis ett löpnummer, och för att förse transaktionsmeddelandet med en digital signatur på basis av nämnda privata nyckel och nämnda asymmetriska algoritm, samt organ för utmatning av det signerade transaktionsmeddelandet.

Enligt en tredje aspekt på föreliggande uppfinning åstadkommes en kombination av ett aktivt kort och en för kommunikation med det aktiva kortet anordnad användarkontrollerad kommunikationsenhet, med vilken kortet är anordnat att sammanföras i och för åstadkommande av ett elektroniskt transaktionsmeddelande, varvid kortet innefattar organ för skyddad lagring av en privat nyckel, organ för lagring av en asymmetrisk algoritm, och processororgan för att förse ett skapat transaktionsmeddelande med en digital signatur baserad på nämnda privata nyckel och nämnda algoritm, och varvid kommunikationsenheten innefattar organ för inmatning av transaktionsuppgifter, varjämte organ är anordnade i kommunikationsenheten och/eller i kortet för att skapa nämnda transaktionsmeddelande.

En fjärde aspekt på föreliggande uppfinning innebär användning av ett aktivt kort med däri lagrad privat nyckel och asymmetrisk kryptoalgoritm för kommunikationsmateberoende åstadkommande i kortet av ett elektroniskt transaktionsmeddelande försett med en på den privata nyckeln baserad digital signatur.

Ytterligare aspekter på särdrag hos uppfinningen kommer att framgå av följande närmare beskrivning av olika utföringsexempel under hänvisning till bifogade ritningar.

Kort beskrivning av ritningarna

Fig. 1 är en schematisk illustration av ett exempel på genomförande av elektroniska transaktioner, under utnyttjande av ett öppet nät, såsom Internet, i enlighet med en uföringsform av föreliggande uppfinning.

Fig. 2 är en schematisk illustration av samma slag som i Fig. 1 exemplifierande alternativa genomföranden av elektroniska transaktioner i enlighet med uppfinningen.

Fig. 3 är en schematisk illustration av ett exempel på genomförande av elektroniska transaktioner, under utyttjande av en butikskortterminal, i enlighet med en anan utföringsform av föreliggande uppfinning.

Fig. 4 är en schematisk illustration av samma slag som i Fig. 3 med ett annat exempel på genomförande av elektroniska transaktioner, under utnyttjande av en butikskortterminal, i enlighet med föreliggande uppfinning.

Fig. 5 är en schematisk illustration av ett exempel på genomförande av elektroniska transaktioner, under utnyttjande av mobil telefoni, i enlighet med annu en utföringsform av föreliggande uppfinning.

Fig. 6 är en schematisk illustration av ett exempel på genomförande av elektroniska transaktioner, under utnyttjande av ett öppet nät för direkt kontakt med en bank, i enlighet med ytterligare en utföringsform av föreliggande uppfinning.

Fig. 7 är en schematisk illustration av exempel på hur ett avancerat aktivt kort kan utnyttjas för genomförande av elektroniska transaktioner i enlighet med föreliggande uppfinning.

Beskrivning av utföringsformer

I Fig. 1 illustreras schematiskt en första utföringsform av uppfinningen, vilken kan användas för kreditkortsbetalning över ett öppet nät, såsom Internet,

mellan en avsändare och en mottagare ingående i ett nätverk. Avsändaren förfogar över ett aktivt kort 1 och en med lämplig kortläsare (antydd vid 2) försedd dator 3, vilken typiskt kan vara en hemdator och vilken har anslutning till Internet 5. En nätverksserver 7 är anluten till nätet 5 samt till i nätverket ingående, olika kreditkortsadministratörer 8 och 9. De senare är på konventionellt sätt anslutna till varandra och till olika kontoförande institutioner, såsom banker 10, 11. I föreliggande exempel antas avsändaren ha konto i banken 10 och ett kreditkort administrerat av administratören 8, under det att mottagaren 12 har konto i banken 11 och ett kreditkort administrerat av administratören 9.

En tillförlitlig tredje part (TTP) 13 är nätverksadministratör och ansvarar för erforderlig nyckelhantering. TTP 13 tilldelar sålunda respektive användare hans privata nyckel, som finns skyddat lagrad i anvandarens kort 1, samt håller en katalog 15 tillgänglig, från vilken respektive användares publika nyckel kan hämtas.

Användarens aktiva kort 1, som även har konventionell kreditkortsfunktion, innehåller på känt sätt minnes- och processororgan i form av en eller flera integrerade kretsar (antydda vid 17), liksom konventionella organ för att möjliggöra kommunikation mellan kortet och en kortläsare, då kortet är placerat i den senare.

Utöver den tidigare nämnda privata nyckeln innehåller nämnda minne- och processororgan en kryptoalgoritm av asymmetrisk typ, vilken kan vara en DES-algoritm, och programvara för genomförande av signering av ett transaktionsmeddelande baserat på den privata nyckeln och nämnda kryptoalgoritm. Det aktiva kortet 1 aktiveras på godtyckligt lämpligt satt, t ex medelst i kortet inmatat PIN eller biometriskt.

Vid genomförande av en transaktion placeras kortet 1 i datorns 3 kortläsare 17 och kortet aktiveras, om så icke skett dessförinnan. Skapandet av ett transaktionsmeddelande kan nu ske i det aktiva kortet 1 och/eller i

datorn 3. Om skapandet sker uteslutande i kortet, vilket ur säkerhetssynpunkt kan vara att föredraga, innehåller kortet också härför lämplig programvara. I detta fall inmatas erforderliga uppgifter för transaktionsmeddelandet (speciellt om belopp och mottagare) via datorns 3 tangentbord in i kortet.

Om själva transaktionsmeddelandet skapas i datorn, har denna försetts med härför erforderlig programvara, som lämpligen levererats till användaren i samband med utgivandet av det aktiva kortet. Inmatning av meddelandeuppgifter sker även här via tangentbordet.

Det är fördelaktigt att som avsändaruppgift använda en kortidentifikation, såsom det aktiva kortets nummer, som ges automatiskt av kortet i samband med skapandet av transaktionsmeddelandet. Som mottagaruppgift kan med fördel inmatas mottagarens kortnummer.

Efter skapandet av transaktionsmeddelandet skall detta förses med ett löpnummer och signeras, vilket såsom nämnts sker i kortet. Om själva meddelandet skapats i kortet kan det för att begränsa den programvara, som måste finnas i kortet, vara önskvärt att utföra den digitala signaturen på själva meddelandet, varvid meddelandet får formen av kryptotext. Det därefter översända signerade meddelandet måste då kunna ge information om avsändaren, så att för äkthetskontroll erforderlig publik nyckel kan inhämtas, såsom kommer att redovisas senare. Speciellt om transaktionsmeddelandet skapas i en skyddad egen dator, kan det vara lämpligt att generera den digitala signaturen på ett kondensat av själva meddelandet, varvid detta senare kommer att föreligga i klartext och också kan översändas i klartext.

Det signerade transaktionsmeddelandet kan nu med fördel ges formen av E-post och därefter sändas över nätet 5 till nätverksservern 7.

Om transaktionsmeddelandet är i klartext, kan servern 7 baserat på uppgifterna i transaktionsmeddelandet utan vidare sända det signare meddelandet antingen till

avsändarens eller mottagarens kortadministratör 8 respektive 9 i och för äkthetskontroll samt, om äkthet konstateras, efterföljande validering, debitering av avsändaren och kreditering av avsändaren av ifrågavarande transktionsbelopp, under utnyttjande av lämplig clearingprocedur.

Äkthetskontrollen innebär att exempelvis avsändarens kortadministratör inhämtar avsändarens publika nyckel från en egen nyckelkatalog eller katalogen 15 hos TTP 13 och med hjälp därav och av ifrågavarande kryptoalgoritm kontrollerar meddelandets digitala signatur.

Om det av servern mottagna meddelandet inte är i klartext, inhämtar servern 7 från katalogen 15 den publika nyckel som hör till den avsändare som kan identifieras av det mottagna, signerade transaktionsmeddelandet, t ex på basis av en särskild avsändaruppgift, såsom en nätverksidentitet eller Internet-identitet. Efter konventionell dekryptering av meddelandet med utnyttjande av den inhämtade publika nyckeln har servern 7 tillgång till meddelandets uppgifter i klartext och kan skicka meddelandet vidare, i och för äkthetskontroll etc, såsom nämnts ovan.

Ännu ett alternativ här är att det på nätet 5 utsända meddelandet förses med en angiven address till behörig kortadministrator, t ex 8, så att servern 7 kan direkt dirigera meddelandet dit för fortsatt behandling enlig ovan. Om det signerade meddelandet icke är i klartext, måste även här det mottagna meddelandet ge sådan information att rätt publik nyckel kan inhämtas i och för äkthetskontroll och dekryptering av själva meddelandet.

I Fig. 2 illustreras schematiskt en andra utföringsform av uppfinningen, som utnyttjar i grunden samma konfiguration som i Fig. 1, ehuru transaktionsmeddelandet från avsändaren sänds direkt till en mottagares dator 21 via nätet 5. Mottagaren sänder meddelandet vidare, vilket kan ske via nätet till servern 7, såsom antytts med pilen 23, eller via någon annan väg, som antyds via pilen 25.

I denna utföringsform kan det vara lämpligt att själva meddelandet är i klartext, så att mottagaren kan se uppgifterna däri, även om han inte har omedelbar tillgång till avsändarens publika nyckel i och för äkthetskontroll eller dekryptering av den digitala signaturen. Det signerade meddelandet kan emellertid av avsändaren vid behov krypteras med en mottagaren tillhörig publik nyckel, varvid mottagaren vid mottagandet dekrypterar meddelandet med utnyttjande av sin egen privata nyckel och tillhörande kryptoalgoritm och därefter vidarebefordrar det dekrypterade men alltjämt signerade meddelandet.

I fallet med en annan transportväg 25 än nätet 5 kan det vara fördelaktigt att utnyttja ett mellanlagringsmedium, t ex en diskett (antydd vid 26), som mottagaren på lämpligt och säkert sätt överlämnar till sin kortadministratör eller bank för fortsatt behandling i enlighet med vad som beskrivits ovan. Det inses att mottagaren kan samla ett antal mottagna transaktionsmeddelanden på ett dylikt mellanlagringsmedium, innan åtgärder för den fortsatta behandlingen vidtages.

I Fig. 3 illustreras schematiskt en utföringsform av uppfinningen som lämpar sig för transaktioner via en främmande "terminal" 31 och som utnyttjar en användarkontrollerad portabel enhet 33 för skapande av ett transaktionsmeddelande.

Enheten 33 utgörs av en kombinerad aktivator och uppgiftsinmatare för det aktiva kortet. Enheten 33 är på lämpligt sätt anordnad för kommunikation med kortet 1, t ex genom att den inbegriper en integrerad kortläsare, i vilket kortet förs in. Enheten 33 har vidare en tangentuppsättning och en display.

Vid betalning exempelvis i en butik placeras kortet i enheten 33 och aktiveras t ex genom att en PIN-kod inmatas medelst enhetens tangentuppsättning. Medelst tangentuppsättningen inmatas dessutom erforderliga betalningsuppgifter, såsom belopp och mottagare. Om transaktionsmeddelandet både skapas och signeras i själva kor-

tet, överförs själva uppgifterna till kortet. Om själva meddelandet och eventuellt ett kondensat därav skall skapas i enheten 33, i och för överföring till och signering i kortet 1, är enheten försedd med processororgan och erforderlig programvara härför.

Kortet med det signerade transaktionsmeddelandet avlägsnas nu från enheten 33 och införs i butikens läsare/terminal 31, varifrån meddelandet sänds för fortsatt behandling på samma sätt som redovisats tidigare. Godkänd äkthetskontroll och validering kan lämpligen innebära att en kvittens sänds tillbaka ill terminalen.

Det inses att terminalen 31 naturligtvis skulle kunna kommunicera med servern 7 på annat sätt än via nätet 5, t ex via en skyddad förbindelse.

I Fig. 4 illustreras en variant av den utföringsform som visas i Fig. 3. Enheten 33 i Fig. 3 är härvid utbytt mot en skyddad, företrädesvis fristående dator eller terminal 43, som kan vara uppställd i exempelvis en butik och möjliggör fristående, säkert skapande av ett transaktionsmeddelande på likartat sätt som beskrivits i anslutning till Fig. 3, i och för inmatning i en butikskortterminal 31.

I Fig. 5 illustreras en utföringsform av föreliggande uppfinning som innebar utnyttjande av en mobiltelefonanordning 51 och ett tillhörande mobiltelenät 55. Mobiltelefonanordningen inbegriper utöver en mobiltelefonfunktion även sådan aktivering- och inmatningsfunktion som beskrivits i samband med enheten 33 i Fig. 3. Mobiltelefonfunktionen är företrädesvis också styrd av det aktiva kortet.

Medelst telefonfunktionen översändes det signerade transaktionsmeddelandet till en enhet eller central 57, som ombesorjer fortsatt behandling av transaktionsmeddelandet exempelvis i enlighet med vad som beskrivits i anslutning till föregående figurer.

Översändandet av transaktionsmeddelandet kan med fördel ske under utnyttjande av en så kallad SMS-tjänst eller liknande hos mobiltelenätet.

Enheten 57 skulle också kunna vara en särskild central, som efter äkthetskontroll etc. ombesörjer betalningar baserat på mottagna transaktionsmeddelanden.

I Fig. 6 illustreras en utföringsform av föreliggande uppfinning som med fördel kan utnyttjas för ombesörjande av betalningsuppdrag. Hos en avsändare, dvs betalare, skapas signerade transaktionsmeddelanden såsom beskrivits, här exemplifierat med samma metod som i Fig. 1. Transaktionsmeddelandet sänds till avsändarens kontoförande bank 10, som i en katalog 60 har tillgång till avsändarens publika nyckel. Det inses att banken skulle kunna vara kortutfärdare och nyckeladministratör och att avsändaruppgiften i transaktionsmeddelandet lämpligen kan utgöras av avsändarens bankkontonummer.

Efter mottagande av ett transaktionsmeddelande och äkthetskontroll därav ombesörjer avsändarens bank 10 genom en clearingprocedur att den i transaktionsmeddelandet lämpligen genom tillhörande bankkontonummer identifierade betalningsmottagaren gottskrivs ifrågavarande belopp, dvs att mottagarens konto i mottagarens bank 11 krediteras beloppet ifråga.

Ett annan alternativ möjlighet är att avsändarens bank 10 sänder en utbetalningsavi direkt till mottagaren 12 exempelvis baserat på mottagaruppgifter i transaktionsmeddelandet. Detta alternativ är antytt medelst den streckade linjen 62 i Fig. 6.

I utförandet enligt Fig. 6 kan det för ökande av säkerheten vara lämpligt att kryptera det översända signerade transaktionsmeddelandet. Avsändaren använder då bankens 10 publika nyckel och företrädesvis samma kryptoalgoritm, som utnyttjas för signeringen. Banken 10 kan såsom inses utan vidare utföra dekryptering med utnyttjande av sin privata nyckel.

Om banken 10 är administratör av avsändarens nyckelpar, dvs besitter såväl den publika nyckel som den privata nyckel som hör till avsändaren, kan avsändaren alternativt utföra krypteringen av det signerade meddelandet med sin publika nyckel. Banken 10 kan då dekryptera det översända meddelandet med utnyttjande av avsändarens privata nyckel, som hämtas från en katalog, innan äkthetskontroll genomförs med utnyttjande av avsändarens publika nyckel.

I Fig. 7 illustreras slutligen schematiskt användning av ett så kallat avancerat aktivt kort i samband med uppfinningen. Det avancerade aktiva kortet 71 har även en tangentuppsättning och en display, som medger att ett signerat transaktionsmeddelande kan skapas i kortet helt och hållet utan externa hjälpmedel. Kortet kan därefter införas i exempelvis en dator eller en terminal i och för vidaresändning av meddelandet och fortsatt behandling i enlighet med vad som beskrivits tidigare.

Ehuru uppfinningen illustrerats genom ett antal utföringsexempel, är uppfinningen självfallet icke inskränkt därtill, utan ändringar och modifikationer är möjliga inom ramen för efterföljande patentkrav. Sålunda kan enskilda särdrag från de olika utföringsexemplen sammanföras i nya kombinationer inom ramen för uppfinningstanken.

PATENTKRAV

1. Förfarande vid genomförande av elektroniska transaktioner, varvid en avsändare av transaktionsmeddelanden tilldelas ett aktivt kort med tillhörande unik identitet och i kortet skyddat lagrad privat nyckel och varvid en tillhörande publik nyckel hålls allmänt tillgänglig, k ä n n e t e c k n a t av att avsändaren i samband med en elektronisk transaktion under egen kontroll, företrädesvis genom egen inmatning av meddelandeuppgifter, skapar ett transaktionsmeddelande, som innehåller för transaktionen erforderliga uppgifter, samt i sitt aktiva kort förser det skapade transaktionsmeddelandet med sin digitala signatur under utnyttjande av sin nämnda privata nyckel i och för senare utmatning och avsändande av transaktionsmeddelandet.

2. Förfarande enligt krav 1, k ä n n e t e c k n a t av att i transaktionsmeddelandet ingår uppgifter om avsändare, mottagare, belopp och företrädesvis ett transaktionslöpnummer.

3. Förfarande enligt krav 1 eller 2, k ä n n e t e c k n a t av att transaktionsmeddelandet skapas fristående fran det kommunikationsnät, som utnyttjas för senare avsändande av transaktionsmeddelandet.

4. Förfarande enligt krav 3, k ä n n e t e c k n a t av att transaktionsmeddelandet skapas off-line.

5. Förfarande enligt nagot av föregående krav, k ä n n e t e c k n a t av att transaktionsmeddelandet skapas i det aktiva kortet.

6. Förfarande enligt krav 5, k ä n n e t e c k n a t av att transaktionsmeddelandet skapas med hjälp av i det aktiva kortet i förväg inlagd programvara och företrädesvis även i kortet i förväg inlagda avsändaruppgifter.

7. Förfarande enligt krav 5 eller 6, k ä n n e t e c k n a t av att för transaktionsmeddelandet erforderliga uppgifter inmatas medelst på det aktiva kortet

anordnade inmatningsorgan, varvid kortet företrädesvis är ett så kallat avancerat aktivt kort.

8. Förfarande enligt något av kraven 1-6, k ä n n e t e c k n a t av att för transaktionsmeddelandet erforderliga uppgifter inmatas medelst en skyddad kortterminal.

9. Förfarande enligt något av kraven 1-6, k ä n n e t e c k n a t av att för transaktionsmeddelandet erforderliga uppgifter inmatas medelst en separat kortkommunikationsenhet, varvid den senare företrädesvis även är en kortaktivator.

10. Förfarande enligt något av kraven 1-6, k ä n n e t e c k n a t av att för transaktionsmeddelandet erforderliga uppgifter inmatas medelst en av det aktiva kortet styrd telekommunikationsenhet, speciellt en mobil sådan, såsom en mobiltelefon.

11. Förfarande enligt något av föregående krav, k ä n n e t e c k n a t av att transaktionsmeddelandet innehåller avsändaruppgift i form av åtminstone en av följande uppgifter: ett kortnummer, ett bankkortnummer, ett betalkortnummer, ett kreditkortnummer, ett kontonummer, ett fakturanummer, och ett ID-nummer.

12. Förfarande enligt något av föregående krav, k ä n n e t e c k n a t av att transaktionsmeddelandet innehåller mottagaruppgift i form av åtminstone en av följande uppgifter: ett kortnummer, ett bankkortnummer, ett betalkortnummer, ett kreditkortnummer, ett kontonummer, ett fakturanummer och ett ID-nummer.

13. Förfarande enligt något av föregående krav, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet sänds till en kort- eller kontoadministratör avseende avsändaren eller mottagaren, att äkthetskontroll av transaktionsmeddelandets digitala signatur sker med utnyttjande av den publika nyckel, som är tilldelad den som av det överförda transaktionsmeddelandet identifieras såsom avsändare, och att mottagaren om äkthet föreligger

gottskrivs transaktionsbeloppet genom en clearing-process.

14. Förfarande enligt krav 13, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet först sänds till mottagaren vilken eventuellt efter egen kontroll av meddelandets digitala signatur vidarebefordrar det signerade transaktionsmeddelandet till nämnda kort- eller kontoadministratör.

15. Förfarande enligt något av kraven 1-12, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet krypteras med utnyttjande av en publik nyckel tillhörande den adressat, vartill transaktionsmeddelandet sänds, att det krypterade signerade transaktionsmeddelandet sänds till adressaten, att adressaten med utnyttjande av sin privata nyckel dekrypterar det signerade transaktionsmeddelandet, att äkthetskontroll av transaktionsmeddelandets digitala signatur sker med utnyttjande av den publika nyckel, som är tilldelad den som av det överförda transaktionsmeddelandet identifieras såsom avsändare, och att mottagaren om äkthet föreligger gottskrivs transaktionsbeloppet genom en clearingprocess.

16. Förfarande enligt krav 15, k ä n n e t e c k n a t av att adressaten är mottagaren, att mottagaren efter dekrypteringen sänder det signerade transaktionsmeddelandet till en kort- eller kontoadministratör, varefter nämnda äkthetskontroll sker.

17. Förfarande enligt något at kraven 1-12, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet krypteras med utnyttjande av avsändarens publika nyckel samt förses med avsändaruppgift och därefter sänds till en kort- eller kontoadministratör, som har avsändarens privata nyckel och som företrädesvis är utfärdare av användarens aktiva kort, att nämnda administratör dekrypterar det mottagna krypterade meddelandet med utnyttjande av nämnda privata nyckel, att äkthetskontroll av det dekrypterade transaktionsmeddelandets digitala signatur sker med utnyttjande av den publika nyckel, som

är tilldelad den som av det överförda transaktionsmeddelandet identifieras såsom avsändare, och att mottagaren om äkthet föreligger gottskrivs transaktionsbeloppet genom en clearingprocess.

18. Förfarande enligt något av kraven 1-14, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet sänds okrypterat, speciellt via ett allmänt kommunikationsnät, såsom Internet eller telekommunikationsnät.

19. Förfarande enligt något av föregående krav, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet sänds såsom E-post.

20. Förfarande enligt något av kraven 1-18, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet sänds via ett mobiltelefoninät, speciellt med utnyttjande av så kallad SMS-tjänst.

21. Aktivt kort för genomförande av elektroniska transaktioner, innefattande organ för lagring av kortidentifieringsuppgifter, organ för skyddad lagring av en privat nyckel, organ för lagring av en asymmetrisk algoritm, organ för inmatning av transaktionsuppgifter i kortet, processororgan för att i kortet skapa ett transaktionsmeddelande baserat på inmatade transkationsuppgifter, såsom uppgifter om belopp och mottagare, och eventuellt i kortet lagrade uppgifter såsom uppgifter om avsändare och företrädesvis ett löpnummer, och för att förse transaktionsmeddelandet med en digital signatur på basis av nämnda privata nyckel och nämnda asymmetriska algoritm, samt organ för utmatning av det signerade transaktionsmeddelandet.

22. Kort enligt krav 21, k ä n n e t e c k n a t av att det är av så kallad avancerad typ.

23. Kombination av ett aktivt kort och en för kommunikation med det aktiva kortet anordnad användarkontrollerad kommunikationsenhet, med vilken kortet är anordnat att sammanföras i och för åstadkommande av ett elektroniskt transaktionsmeddelande, varvid kortet innefattar

organ för skyddad lagring av en privat nyckel, organ för lagring av en asymmetrisk algoritm, och processororgan för att förse ett skapat transaktionsmeddelande med en digital signatur baserat på nämnda privata nyckel och nämnda algoritm, och varvid kommunikationsenheten innefattar organ för inmatning av transaktionsuppgifter, varjämte organ är anordnade i kommunikationsenheten och/eller i kortet för att skapa nämnda transaktionsmeddelande.

24. Kombination enligt krav 23, k ä n n e t e c k n a t av att kommunikationsenheten är en mobil telekommunikationsanordning.

25. Kombination enligt krav 23, k ä n n e t e c k n a t av att kommunikationsenheten är en kombinerad kortaktivator och uppgiftsinmatare/behandlare.

26. Användning av ett aktivt kort med däri lagrad privat nyckel för kommunikationsnätoberoende åstadkommande av ett elektroniskt transaktionsmeddelande försett med en på den privata nyckeln baserad digital signatur.

SAMMANDRAG

Förfarande och anordning för genomförande av elektroniska transaktioner. En avsändare skapar under full egen kontroll ett transaktionsmeddelande i ett aktivt kort (1) och förser meddelandet med sin digitala signatur i kortet i och för senare utmatning och avsändande.

(Fig. 1)

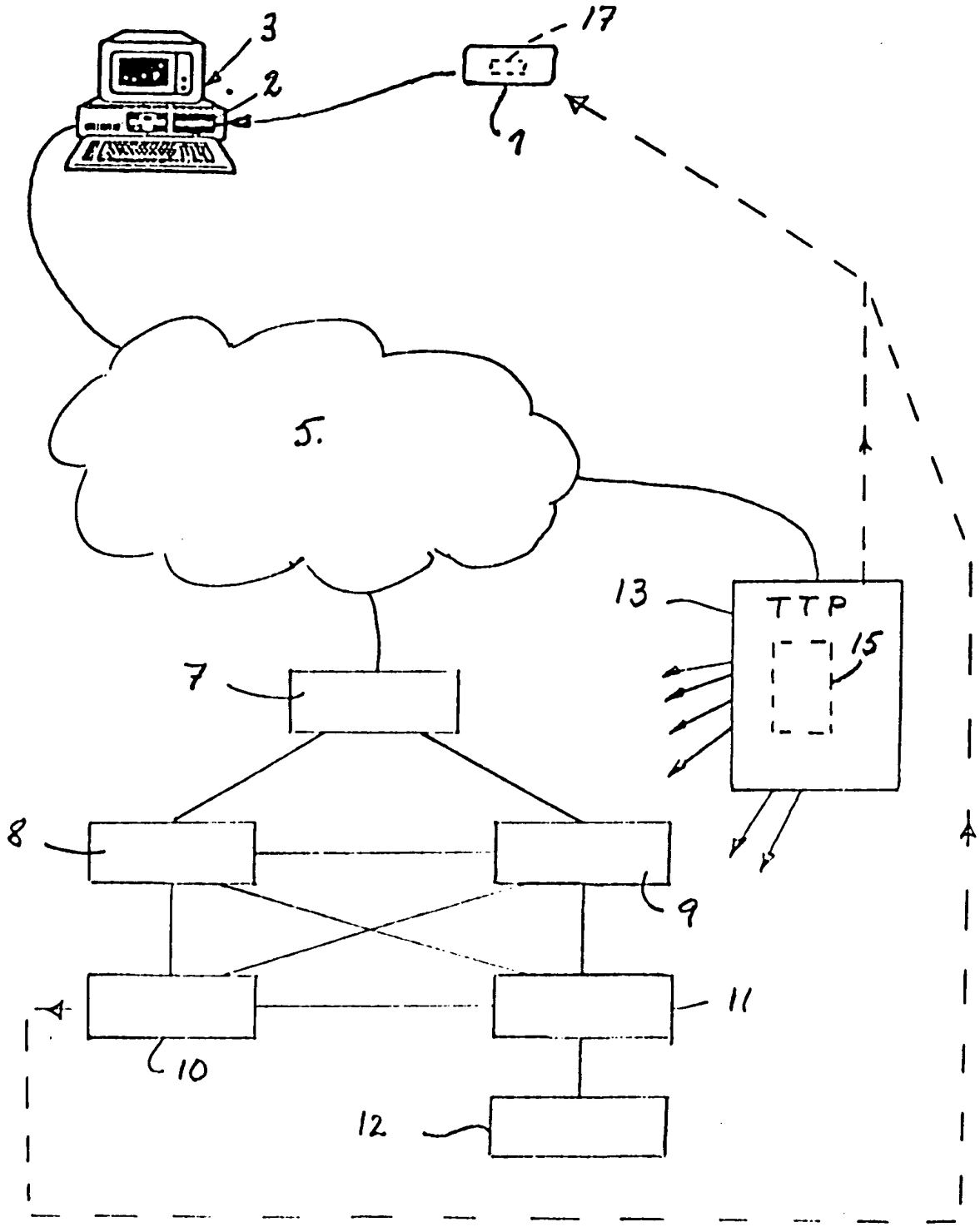

Fig. 1

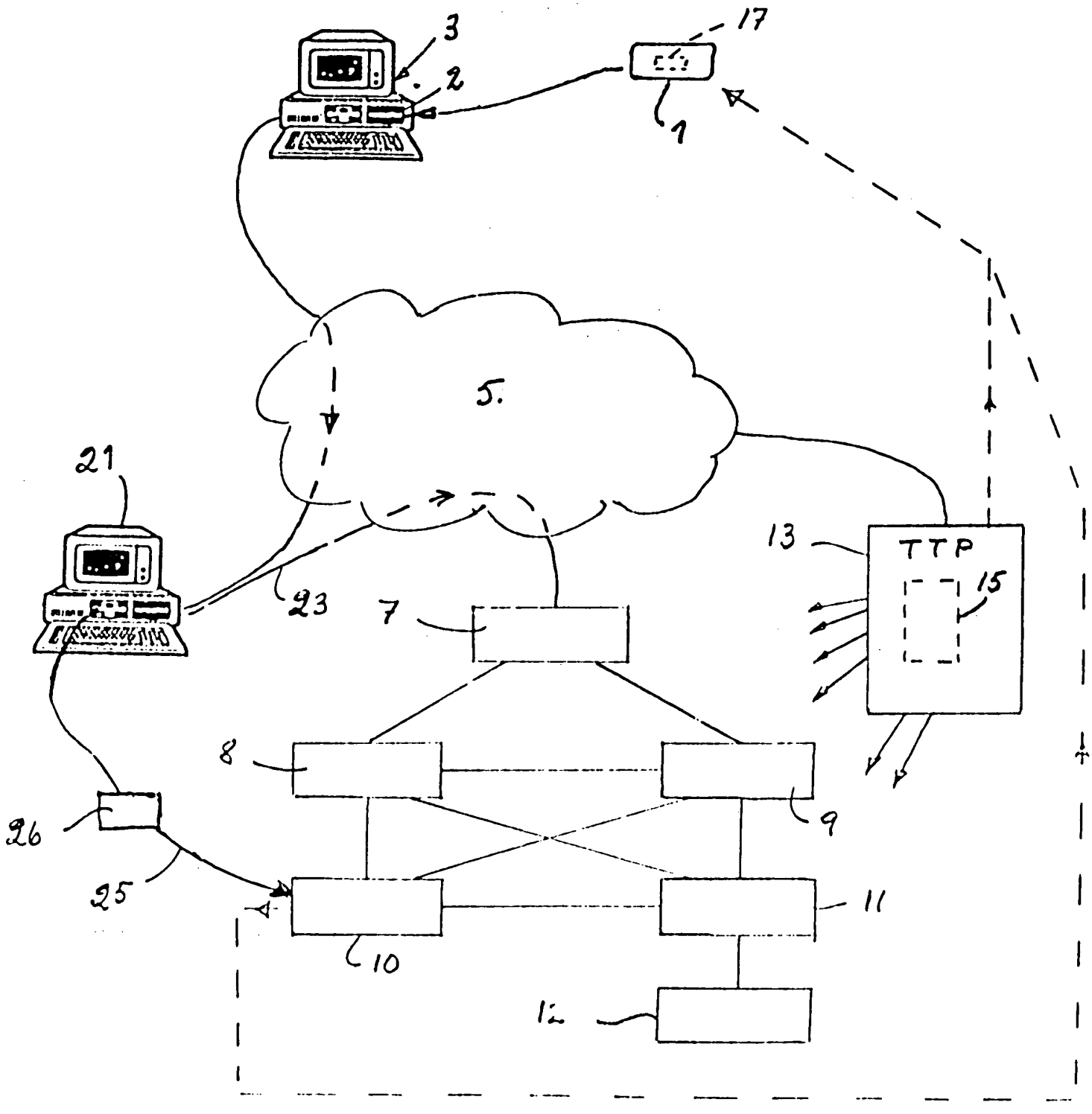

Fig. 2

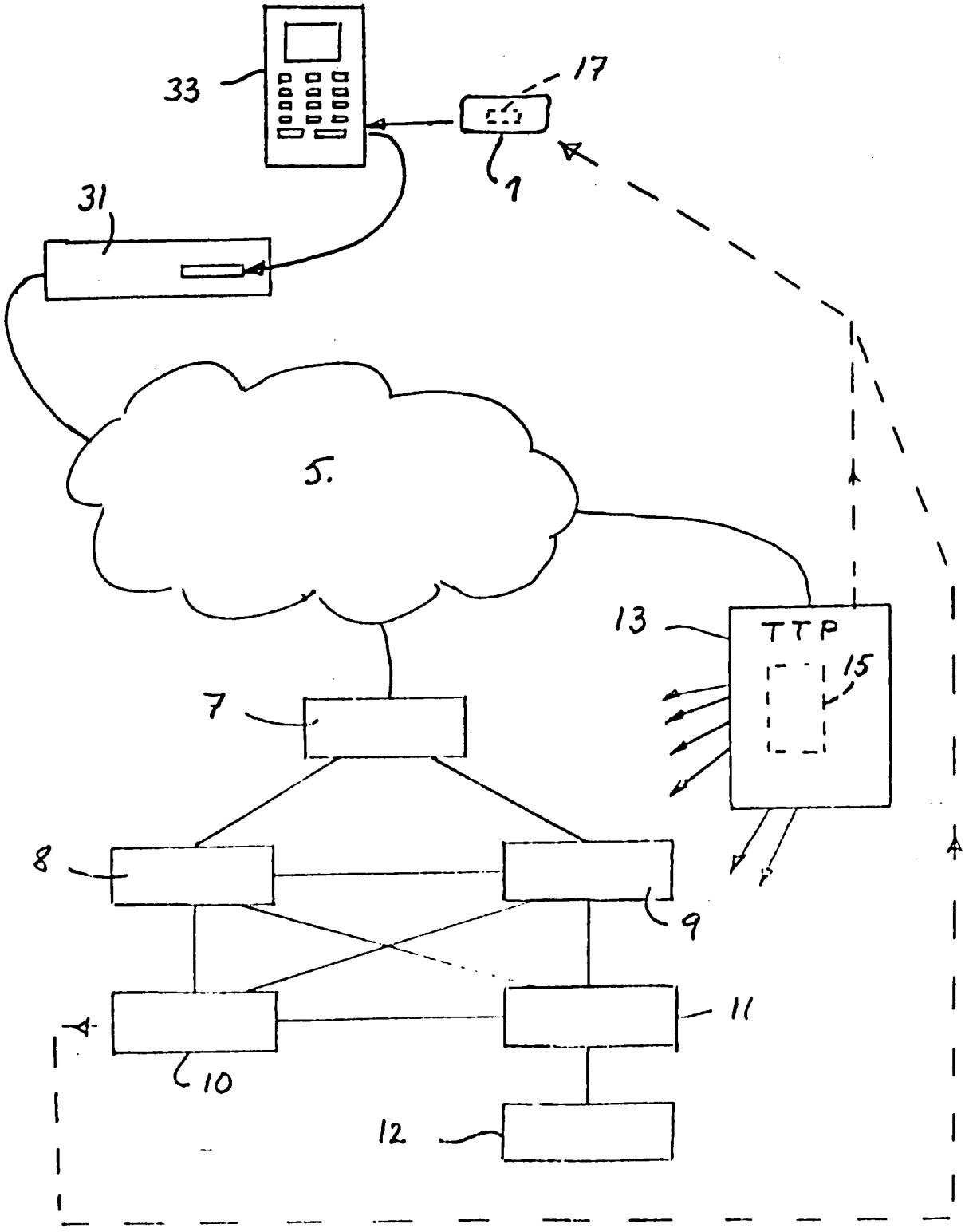

Fig. 3

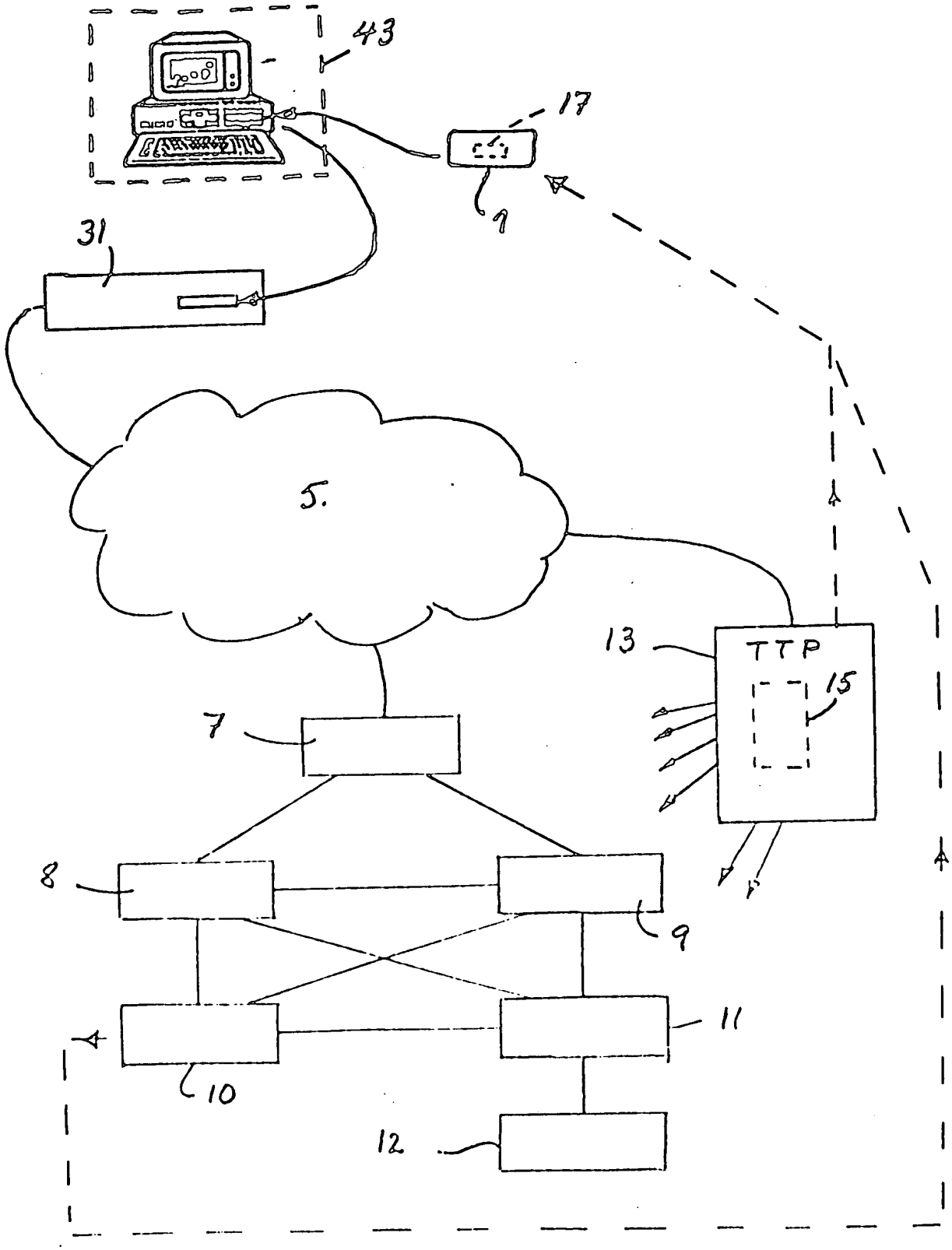

Fig. 4

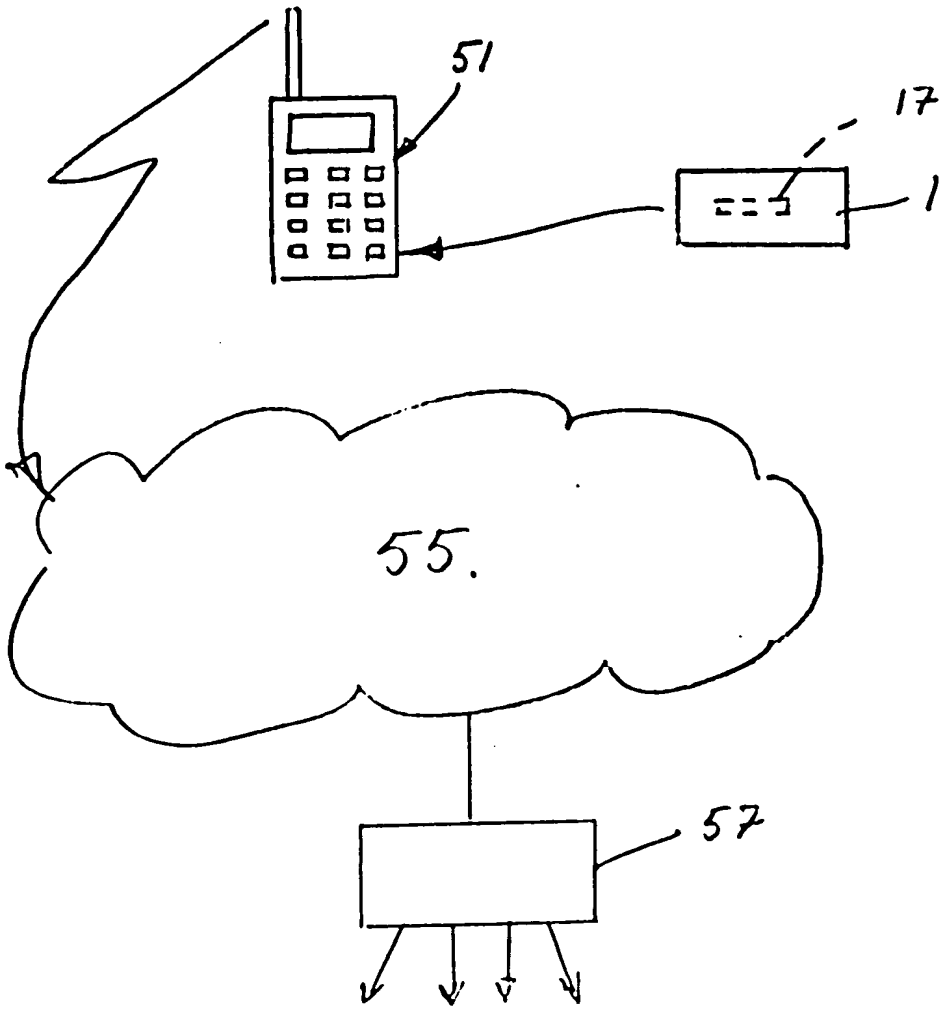

Fig. 5

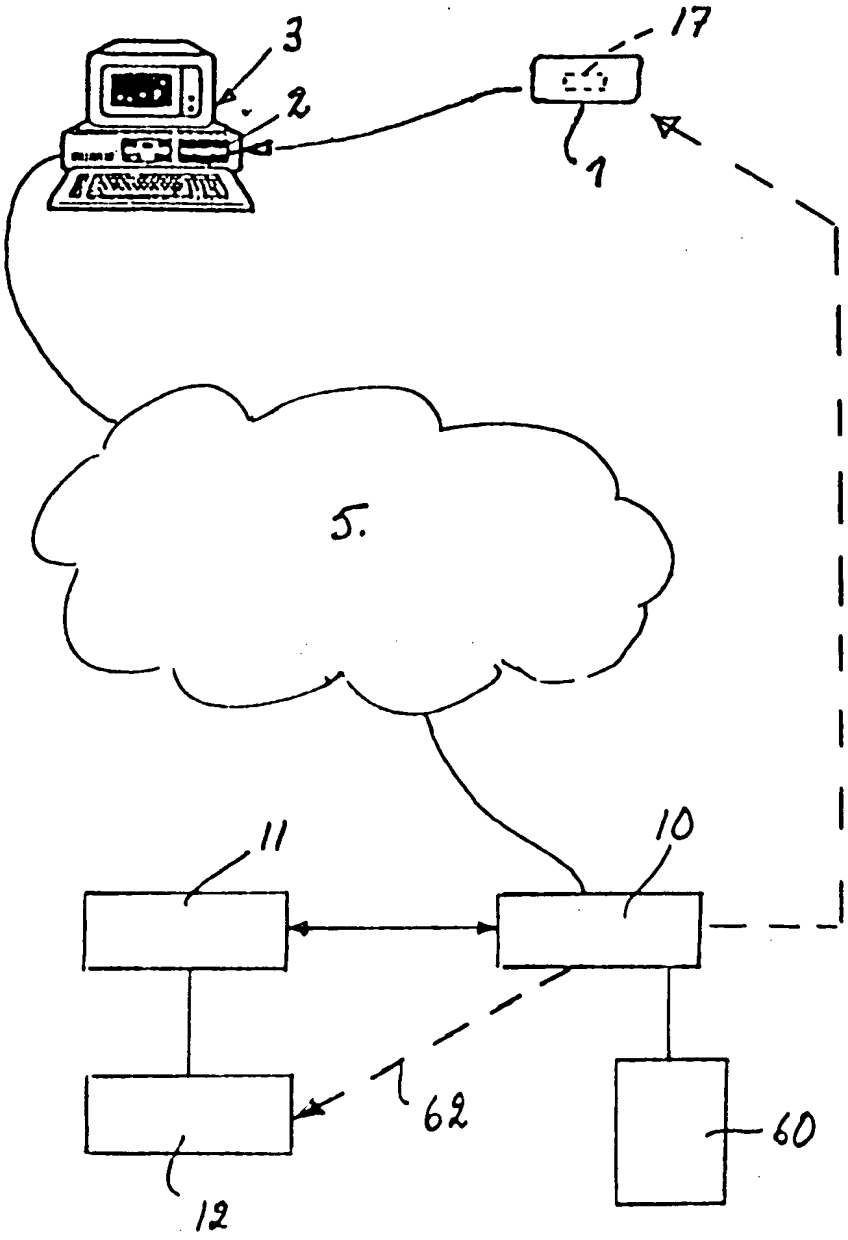

Fig. 6

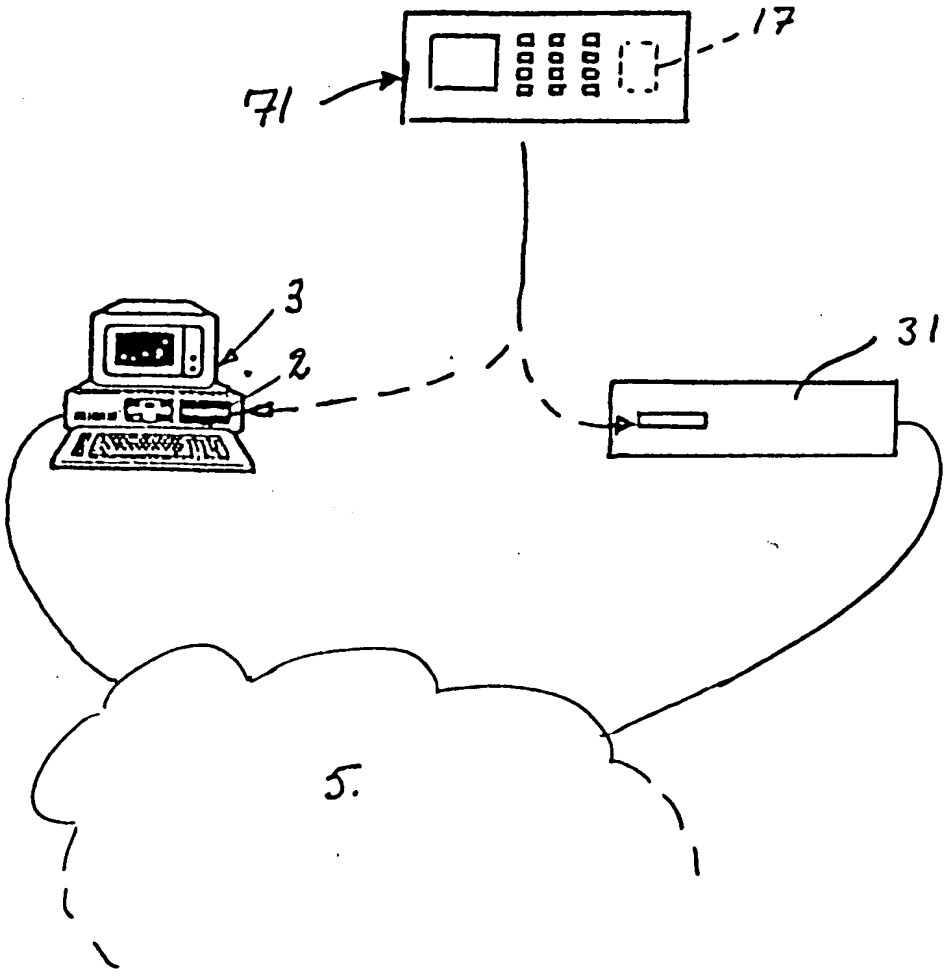

Fig. 7